REMARKS

Claims 1 - 16 are pending. In reply to the Office Action mailed July 12, 2005, Applicant requests consideration of the following remarks and timely allowance of all pending claims.

Claim Rejections under 35 U.S.C. § 103

The Examiner rejected claims 1-16 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,321,752 to Iwamura et al. ("Iwamura"), and further in view of Sathi Perumal "Pipelined 50 MHz CMOS ASIC for 32 bit binary to residue conversion," 1994 ("Perumal"). Applicants respectfully traverse.

With regard to claim 1, the Examiner wrote that Iwamura teaches "a modular communication apparatus [col. 6 lines 5 -9 'which performs encryption or decryption of a communication content by using a modular exponentiation...the communication apparatus comprising'] which utilizes a residue number system [col 3. lines 50-53 'modular exponentiation and modular multiplication employed in cryptic communication is executed simply by repeating modular multiplication using R which is prime to N which is the residue']". *See* Office Action, pg. 2. The Examiner further wrote that "Iwamura teaches the apparatus comprising four various processing unit (i.e. four various computing means col. 6 lines 19-32). *See* Office Action, pg. 4. Applicants respectfully disagree with these characterizations of Iwamura and traverse the rejection as follows.

Claim 1 recites "a first processing unit configured to obtain a residue number system representation of a value Cp^{dp} x B mod p or a value with p added thereto based on a residue number system representation of a remainder value Cp = C mod p by p of said data C ...; a second processing unit configured to obtain a residue number system

representation of a value $cq^{dq} \times B \bmod q$ or a value with q added thereto based on a residue number system representation of a remainder value $Cq = C \bmod q$ by q of said data C ...; a third processing unit configured to obtain a residue number system representation of an integer m' congruent with $C^d \bmod (p \times q)$ based on both the residue number system representations obtained by said first and second processing units; and a fourth processing unit configured to obtain said calculation result ... by converting said residue number system representation obtained by said third processing unit into a binary representation."

In contrast, Iwamura does not utilize residue number system ("RNS") representations. Iwamura aims to provide a method and apparatus that enables a circuit of a small circuit scale to perform the high-speed modular multiplication or modular exponentiation used for encryption and decryption in cryptic communication *See*, Iwamura Abstract. In Iwamura, the modular exponentiation and modular multiplication employed in cryptic communication are executed simply by repeating the modular multiplication using R, which is prime to the residue N (col. 3, lines 50-53). Although Iwamura states that integer R is prime to residue N, Iwamura does not use an RNS representation of R. In Iwamura, encryption and decryption are accomplished using the modular multiplication of two integers A and B, expressed as A*B mod N, and through modular exponentiation which is expressed by $C = M^e \bmod N$(C, M, N, e). Modular exponentiation is accomplished by repeating the modular multiplication process. See Iwamura, col. 1, lines 13-24. Therefore, contrary to the Examiner's assertion, Iwamura does not teach a modular exponentiation calculation apparatus utilizing residue number system representations, as recited in claim 1.

Furthermore, Iwamura does not teach or suggest the use of a fourth processing unit to convert an RNS representation into binary as asserted by the Examiner. As the Examiner concedes Iwamura does not teach the calculation of a result by converting a RNS representation to binary. Because Iwamura does not calculate values expressed in an RNS representation, the apparatus in Iwamura neither needs nor includes a fourth unit configured to convert the residue number system representation obtained by the third processing unit into a binary representation.

Perumal does not cure deficiencies of Iwamura. Perumal teaches the calculation of a binary number from two residue numbers (See Perumal equation 13) but does not teach or suggest a modular exponentiation calculation apparatus utilizing a residue number system, or the use of a fourth processing unit to convert an RNS representation into binary, as recited by claim 1.

Furthermore, because Iwamura does not calculate values expressed in an RNS representation, Iwamura does not need an RNS-to-binary converter. Therefore, there is no motivation to combine the teachings in Iwamura with the teachings in Perumal, and the teachings, if combined would not yield the present invention.

Claims 2 - 13 depend from claim 1 and are also patentable for at least the same reasons as is claim 1. Independent claims 14, 15 and 16 recite a method, article of manufacture, and decryption apparatus that recite elements substantially similar to those found in claim 1 and, in fact, were rejected by the Examiner for the same reasons as claim 1. See Office Action, pg. 12. Applicants submit that these claims are patentable over the combination for the reasons stated above with respect to claim 1.

In view of the foregoing remarks, Applicants request reconsideration of these remarks, and timely allowance of the pending claims.

Please grant any extensions of time required to enter this response and charge any additional required fees to our deposit account 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, L.L.P.

Dated: December 12, 2005

By: _____

Venk Krishnamoorthy, Ph.D.
Reg. No. 52,490